[rev. 06/14/2000]

National Infrastructure Protection Center

Cyber Threat and Computer Intrusion
Incident Reporting Guidelines

This form may be used as a guide or vehicle for reporting cyber threat and computer intrusion incident information to the NIPC or other law enforcement organization. It is recommended that these ***Cyber Incident Reporting Guidelines*** be used when submitting a report to a local FBI Field Office.

Do NOT include **CLASSIFIED** information on this form unless you adhere to applicable procedures for proper marking, handling and transmission of classified information. Please contact NIPC Watch Operations Center (202) 323-3205 to arrange secure means to submit classified information.

Information concerning the identity of the reporting agency, department, company, or individual(s) will be treated on a confidential basis. If additional information is required, you will be contacted directly.

Report Date/Time: _____

When completed, fax to NIPC WWU (202) 323-2079/2082.

SECTION 1

Point of Contact (POC) Information

Name:

Title:

Telephone/Fax number:

E-mail:

Organization:

Address: Street _____

City, State, Zip Code _____

Country _____

SECTION 2

Incident Information

1. Name of organization: (if same as above, enter "SAME")

❑ (Check here if Federal Government Agency)

Organization's contact information:

Telephone number:

Address: (if same as above, enter "SAME")

Street _____

City, State, Zip Code _____

Country_____

E-mail: _____

2. Physical Location(s) of victim's computer system/network (Be Specific):

3. Date/time and duration of incident: _____.

4. Is the affected system/network critical to the organization's mission?

❑ Yes ❑ No

5. Critical infrastructure sector(s) affected. (Check all that apply)

❑	Power	❑	Transportation
❑	Banking and Finance	❑	Emergency Services
❑	Government Operations	❑	Water Supply Systems
❑	Gas & Oil Storage and Delivery	❑	Other (Provide details in remarks)
❑	Telecommunications	❑	Not applicable

Remarks:

6. Nature of Problem? (Check all that apply)

- ❑ Intrusion
- ❑ Unauthorized root access
- ❑ Compromise of system integrity
- ❑ Theft
- ❑ Unknown
- ❑ System impairment/denial of resources
- ❑ Web site defacement
- ❑ Hoax
- ❑ Damage
- ❑ Other (Provide details in remarks)

7. Has this problem been experienced before? (If yes, please explain in remarks section):

- ❑ Yes
- ❑ No

Remarks:

8. Suspected method of intrusion/attack

- ❑ Virus (provide name if known)
- ❑ Denial of Service
- ❑ Distributed Denial of Service
- ❑ Unknown
- ❑ Vulnerability exploited (explain)
- ❑ Trojan horse
- ❑ Trapdoor
- ❑ Other (Provide details in remarks)

Remarks:

9. Suspected perpetrator(s) or possible motivation(s) of the attack

- ❑ Insider / Disgruntled employee
- ❑ Competitor
- ❑ Unknown
- ❑ Former employee
- ❑ Other (Explain in remarks)

Remarks:

10. The apparent source (IP address) of the intrusion/attack: _____

11. Evidence of spoofing?

- ❑ Yes
- ❑ No
- ❑ Unknown

12. What computers/systems (hardware and software) were affected? (Operating system, version):

- ❑ Unix
- ❑ Linux
- ❑ NT
- ❑ Sun OS/Solaris
- ❑ OS2
- ❑ VAX/VMS
- ❑ Windows
- ❑ Other (Please specify in remarks)

Remarks:

13. Security Infrastructure in place. (Check all that apply)

- ❑ Incident/Emergency Response Team
- ❑ Firewall
- ❑ Intrusion Detection System
- ❑ Security Auditing Tools
- ❑ Packet filtering
- ❑ Encryption
- ❑ Secure Remote Access/Authorization tools
- ❑ Banners
- ❑ Access Control Lists

14. Did the intrusion/attack result in a loss/compromise of sensitive, classified or proprietary information?

- ❑ Yes (Provide details in remarks)
- ❑ No
- ❑ Unknown

Remarks:

15. Did the intrusion/attack result in damage to system(s) or data?

- ❑ Yes (Provide details in remarks)
- ❑ No

Remarks:

16. What actions and technical mitigation have been taken?

- ❑ System(s) disconnected from the network?
- ❑ Backup of affected system(s)
- ❑ Log files examined
- ❑ System Binaries checked
- ❑ Other (Please provide details in remarks)
- ❑ No action(s) taken

17. Has the local FBI field office been informed?

❑ Yes (Which office) ❑ No

18. Has another agency/organization been informed? If so, please provide name and phone number.

❑ Yes ❑ No

- State/local police
- Inspector General
- CERT-CC
- FedCIRC
- JTF-CND
- Other (Incident Response, law enforcement, etc.)

19. When was the last time your system was modified or updated?

Date:_____

Company/Organization that did work (Address, phone, POC information): _____

_____

20. Is the System Administrator a contractor?

❑ Yes (Provide POC information ❑ No

_____

21. In addition to being used for law enforcement or national security purposes the intrusion-related information I have reported may be shared with:

❑ The Public

❑ InfraGard Members with Secure Access

22. Additional Remarks: (Please limit to 500 characters. Amplifying information may be submitted separately.)

If the reported incident is determined to be a criminal matter you may be contacted by an agent for additional information**.**